Der Lucas–Lehmer Test

Michael E. Pohst <pohst@math.tu-berlin.de>

Dieser Vortrag wird gehalten am 12. Juni 2004 anläßlich der Langen Nacht der Wissenschaften
http://www.math.tu-berlin.de/~kant/mersenne.html

10. Juni 2004

1 Mersennsche Primzahlen

Zu einer natürlichen Zahl n wird die zugehörige Mersennezahl M_n als $M_n = 2^n - 1$ definiert.

Für $n = 2,\ 3,\ 5,\ 7,\ 13$ ist M_n eine Primzahl.

Merke:
Ist M_n eine Primzahl, so ist notwendig n eine Primzahl.

Die Umkehrung hiervon ist nicht richtig, wie das Beispiel $n = 11$ mit $2^{11} - 1 = 23 \cdot 89$ lehrt.

Die Bedeutung der Mersenneschen Zahlen liegt hauptsächlich darin, dass man selbst für große Primzahlen n relativ schnell feststellen kann, ob M_n Primzahl ist oder nicht.

2 Der Lucas–Lehmer Test

Zu vorgegebener Primzahl n setzt man:

$s_0 := 4$

und berechnet nacheinander für

$k = 0, 1, 2, ..., n-2$:

$$s_{k+1} := s_k^2 - 2. \qquad \textbf{(LL-Folge)}$$

M_n ist genau dann eine Primzahl, wenn s_{n-2} durch M_n teilbar ist.

3 Teilbarkeit und prime Restklassengruppen

In den ganzen Zahlen $\mathbb{Z}$ gibt es die Division mit Rest:

Zu $a, m \in \mathbb{Z}$ mit $m \neq 0$ existieren stets – und zwar eindeutig – ein Quotient $Q = Q(a, m)$ und ein Rest $R = R(a, m)$ mit $a = Qm + R$ und $0 \leq R < |m|$.

Im Folgenden sei $m \geq 2$ stets eine ganze Zahl.

Auf der Menge $\{0, 1, ..., m-1\}$ lässt sich mittels $x \cdot y := R(xy, m)$ eine Multiplikation erklären, die mit den üblichen Rechenregeln verträglich ist.

Beispiel: Für $m = 5$ wird
$0 \cdot i = 0\ \ (0 \leq i \leq 4),\ 1 \cdot i = i\ \ (1 \leq i \leq 4),\ 2 \cdot 2 = 4,\ 2 \cdot 3 = 1,\ 2 \cdot 4 = 3,\ 3 \cdot 3 = 4,\ 3 \cdot 4 = 2,\ 4 \cdot 4 = 1$.

Mathematisch gesehen rechnet man in dem Restklassenring $\mathbb{Z}/m\mathbb{Z}$, die Restklassen werden durch Vertreter repräsentiert. Der Einfachheit halber schreiben wir auch -1 an Stelle von $m-1$.

Im folgenden bezeichne T_m die Teilmenge der Zahlen $j \in \{1, ..., m-1\}$, die zu m teilerfremd sind. Dann wird T_m mit der oben erklärten Multiplikation zu einer endlichen kommutativen Gruppe mit $\phi(m)$ Elementen. $((\mathbb{Z}/m\mathbb{Z})^\times)$

Beispiel: Ist m eine Primzahl, so gilt $\phi(m) = m-1$, T_m ist **zyklisch**, wird also von einem geeigneten Element q aus T_m erzeugt: $T_m = \{q, q^2, ..., q^{m-1}\}$.

T_5 besteht aus den Elementen $2^1 = 2$, $2^2 = 4$, $2^3 = 3$, $2^4 = 1$.

4 Prime Restklassengruppen und quadratische Reste

Für $x \in T_m$ heißt jedes $k \in \mathbb{Z}$ mit $x^k = 1$ **Exponent** von x.

Wie man leicht einsieht, existiert stets ein minimaler positiver Exponent, die **Ordnung** $|(|\, x)$.

Wichtige Eigenschaften:

Die Elementzahl $\phi(m)$ ist Exponent für jedes $x \in T_m$. Es folgt $x^{\phi(m)+1} = x$. (**A1**)

$|(|\, x)$ teilt jeden Exponenten von x. (**A2**)

Beispiel: Ist $|(|\, x) = 6$, so folgt $|(|\, x^2) = 3$.

$x \in T_m$ heißt **quadratischer Rest** zu m, falls es ein $y \in T_m$ mit $x = y^2$ gibt.

Beispiel: Es sei m eine ungerade Primzahl und $T_m = \langle q \rangle = \{q, q^2, ..., q^{m-1}\}$. Dann sind genau die geraden Potenzen von q quadratische Reste.

$-1 = m-1$ ist genau dann quadratischer Rest zur Primzahl m, falls $R(m, 4) = 1$ ist. (**A3**)

2 ist genau dann quadratischer Rest zu m, wenn $R(m, 8) = 1$ oder $R(m, 8) = 7$ ist.
(Beachte: $T_8 = \{1, 3, 5, 7\}$.) (**A4**)

Gilt $m \neq 3$, so gilt $R(3^{(m-1)/2}, m) = 1$ für $R(m, 12) \in \{1, 11\}$ und $R(3^{(m-1)/2}, m) = -1$ für $R(m, 12) \in \{5, 7\}$.
(Quadratisches Reziprozitätsgesetz) (**A5**)

5 Höhere prime Restklassengruppen und quadratische Reste

Es ist $T := \{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ ein kommutativer Ring. T enthält die Elemente $\psi = 2 + \sqrt{3}$ und $\bar{\psi} = 2 - \sqrt{3}$. Man rechnet leicht nach:

$$\psi\bar{\psi} = 1; \tag{A6}$$

Die Elemente der LL-Folge genügen (A7)
$s_k = \psi^{2^k} + \bar{\psi}^{2^k}$ $(k = 0, 1, 2, ...)$
(per vollständiger Induktion nach k).

Es sei m eine Primzahl, für die 3 kein quadratischer Rest ist. Dann wird (A8)

$$T_m := \{a + b\sqrt{3} \mid 0 \le a < m,\ 0 \le b < m,\ a + b > 0\}$$

mit der üblichen Multiplikation und anschließender Reduktion der Koeffizienten auf ihre Reste bei Division durch m zu einer kommutativen multiplikativen Gruppe mit $m^2 - 1$ Elementen.

Mathematisch gesehen entspricht T_m der primen Restklassengruppe $(T/mT)^\times$. Zum Rechnen in T bzw. T_m:

$$\begin{aligned} R((a + b\sqrt{3})^m, m) &= R\left(\textstyle\sum_{i=0}^{m} \binom{m}{i} a^{m-i}\sqrt{3}^i b^i,\ m\right) \\ &\quad \text{(binomische Formel)} \\ &= R(a^m + b^m\sqrt{3}^m,\ m) \\ &\quad \left(\text{da } R\left(\tbinom{m}{i},\ m\right) = 0 \text{ für } 1 \le i < m\right) \\ &= R(a + b3^{(m-1)/2}\sqrt{3},\ m) \ \text{(nach (A1))} \\ &= R(a - b\sqrt{3},\ m) \ \text{(wegen (A5))}. \end{aligned} \tag{A9}$$

Ist 2 ein Quadrat in $\{1, 2, ..., m-1\}$ (also erst recht in T_m), etwa $2 = x^2$, (A10)
so gilt in T_m:

$$2 + \sqrt{3} = R\left(\left(\tfrac{1+\sqrt{3}}{x}\right)^2,\ m\right).$$

6 Beweis von Lucas–Lehmer (Implikation)

Es seien $n \ge 3$ sowie $M_n = 2^n - 1$ Primzahlen.

Speziell ist dann $R(M_n, 8) = 7$, siehe (A4). Ferner ist 3 kein quadratischer Rest zu M_n gemäß (A5).

Wir wissen nach (A6) und (A7):

Die Elemente der LL-Folge genügen **(A11)**

$$s_{n-2} \;=\; \psi^{2^{n-2}} + \bar{\psi}^{2^{n-2}} \;=\; \bar{\psi}^{2^{n-2}}(1+\psi^{2^{n-1}})\;.$$

Damit M_n die Zahl s_{n-2} teilt, reicht wegen (A11) der Nachweis von $R(\psi^{2^{n-1}},\, M_n) = -1 (= M_n - 1)$.

Unter Ausnutzung von

$$2^{n-1} = (M_n+1)/2$$

und

$$R(2^{(M_n-1)/2},\, M_n) = 1$$

(wegen (A4)) erhalten wir:

$$\begin{aligned}
R(\psi^{2^{n-1}},\, M_n) &= R\left(2^{(M_n-1)/2}\Big(\frac{1+\sqrt{3}}{x}\Big)^{M_n+1},\, M_n\right) \\
&\quad \text{(wegen (A10))} \\
&= R\left(\frac{1+\sqrt{3}}{2}(1+\sqrt{3})^{M_n},\, M_n\right) \\
&\quad \text{(wegen (A10))} \\
&= R\left(\frac{1+\sqrt{3}}{2}(1-\sqrt{3}),\, M_n\right) \\
&\quad \text{(wegen (A9) und (A5))} \\
&= -1\;(= M_n - 1)\;.
\end{aligned}$$

7 Beweis von Lucas–Lehmer (Umkehrung)

Wir setzen jetzt voraus, dass s_{n-2} durch M_n teilbar ist (in $\mathbb{Z}$). Dann wird auch $\psi^{2^{n-2}} s_{n-2}$ von M_n geteilt (in T). Hiernach ist

$$R(1+\psi^{2^{n-1}},\, M_n) = 0 \quad \text{also} \quad R(\psi^{2^n},\, M_n) = 1 \qquad \textbf{(A12)}$$

Es sei nun q ein beliebiger Primfaktor von M_n. (Notwendigerweise gilt $q \neq 2$ und $q \neq 3$.) Dann gilt (A12) auch bei Division durch q an Stelle von M_n.

Wegen der speziellen Gestalt der Exponenten folgt, dass 2^n die Ordnung von ψ in der multiplikativen Gruppe

$$T_q \;:=\; \{a + b\sqrt{3} \mid 0 \le a < q,\; 0 \le b < q,\; a+b > 0\}$$

ist. Ist also k ein Exponent von ψ in dieser Gruppe, das heißt gilt $R(\psi^k, q) = 1$, so folgt gemäß (A2), dass k von (der relativ großen Zahl) 2^n geteilt wird.

Wir nutzen dies aus, um zu zeigen, dass dann M_n notwendig mit der Primzahl q übereinstimmt. Dabei haben wir zwei Fälle zu unterscheiden (vgl. (A5)).

1. Fall: $\sqrt{3}$ ist ein Quadrat in T_q.

$$\begin{aligned} R(\psi^{q-1}, q) &= R((2-\sqrt{3})(2+\sqrt{3})^q,\, q) \ \text{(wegen (A6))} \\ &= R((2-\sqrt{3})(2+\sqrt{3}),\, q) \ \text{(wegen (A5))} \\ &= 1\,. \end{aligned}$$

Nach den Vorbemerkungen ist demnach $q-1$ ein Vielfaches von 2^n, etwa $2^n h = q-1$ mit $h \geq 1$. Aber dann folgt

$$q = 2^n h + 1 > 2^n - 1 = M_n$$

im Widerspruch dazu, dass q ein Teiler von M_n sein sollte. Dieser Fall tritt also nicht auf.

2. Fall: $\sqrt{3}$ ist kein Quadrat in T_q.

$$\begin{aligned} R(\psi^{q+1}, q) &= R((2+\sqrt{3})(2+\sqrt{3})^q,\, q) \\ &= R((2+\sqrt{3})(2-\sqrt{3}),\, q) \ \text{(wegen (A5))} \\ &= 1\,. \end{aligned}$$

Nach den Vorbemerkungen ist in diesem Fall $q+1$ ein Vielfaches von 2^n, etwa $2^n h = q+1$ mit $h \geq 1$. Wir erhalten hier
$q = 2^n h - 1 \geq 2^n - 1 = M_n$.

Da q als Teiler von M_n angenommen war, muss notwendig $h = 1$ und somit $q = M_n$ gelten. Da aber q Primzahl war, ist auch M_n eine Primzahl.